ly

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,265	08/01/2001	Warwick Ford	21190-05339	8690

758 7590 02/11/2005

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/921,265	**Applicant(s)** FORD, WARWICK	
	Examiner Matthew T Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 October 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3 IDS*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 8/1/2001.

DETAILED ACTION

1. Claims 1-19 have been examined.

Title

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Priority

3. The application has been filed under Title 35 U.S.C §119(e), claiming priority to Provisional application 60/226,429, filed August 18, 2000.

4. The effective filing date for the subject matter defined in the pending claims in this application is 8/18/2000.

Information Disclosure Statement

5. The information disclosure statements (IDS) submitted on 12/31/2001, 10/08/2002, and 10/16/2002 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on 10/01/2001 are acceptable for examination proceedings.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "bona fides" in claim 3 appears to be used by the claim to mean "something of the clients that can be checked", while the accepted meaning is "authentic." The term is indefinite because the specification does not clearly redefine the term. Because the ordinary person would not be able to determine what constitutes "bona fides", the ordinary person skilled in the art would not be able to determine the scope of the claim. Therefore, claim 3 is rejected for failing to point out and distinctly claim the subject matter which the applicant regards as the invention.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.*

10. Claims 1, 5-8, and 16-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Fielder et al. (US Patent Number 5,995,624) hereinafter referred to as Fielder.

11. Regarding claim 1, Fielder disclosed a method for validating a client device (Originating System) by a server device (Answering System) (See Fielder Abstract), said method comprising the steps of: generating a shared unpredictable secret (See Fielder Col. 9 Paragraph 1 wherein the unpredictable secret is the dynamic secret); storing the shared unpredictable secret client device (See Fielder Col. 9 Lines 10-12) and in the server device (See Fielder Col. 10 Lines Paragraph 6); requiring the client device to prove that it holds a correct secret precondition to the server device validating the client device (See Fielder Fig. 4b Steps 214-217 and Col. 10 paragraphs 4-6); and replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device (See Fielder Col. 9 Lines 10-12 and Col. 10 paragraph 6).

12. Regarding claim 5, Fielder disclosed that the shared unpredictable secret is generated by a generator from the group comprising a random number generator and a pseudo-random number generator (See Fielder Col. 6 Paragraph 9).

13. Regarding claim 6, Fielder disclosed that the shared unpredictable secret comprises an unpredictable component and a fixed component (See Fielder Col. 9 Lines 5-10 and Col. 6 Paragraph 9).

14. Regarding claim 7, Fielder disclosed that a plurality of devices desire to be validated by the server device; and each client device has a unique unpredictable secret that it shares with the server device (See Fielder Col. 13 Paragraphs 2-3).

15. Regarding claim 8, Fielder disclosed that following a validation of the client device, the server device discards the original shared unpredictable secret and stores within server device a new shared unpredictable secret that can be generated by applying update data to the original shared unpredictable secret (See Fielder Col. 10 Paragraph 6 and Col. 6 paragraph 3).

16. Regarding claim 16, Fielder disclosed that the client device presents proof data to the server device, wherein the proof data are derived from a shared unpredictable secret using a proof data generation algorithm, and the proof data do not divulge the shared unpredictable secret (See Fielder Col. 8 Lines 15-67); the server device checks the proof data by using a proof data generation algorithm consistent with the proof data generation algorithm used by the client device (See Fielder Col. 10 Lines 38-62); and when the server device determines that the proof data presented by the client device were not generated from the same shared unpredictable secret that is stored in both the client device and in the server device, the server device does not validate the client device (See Fielder Col. 10 Lines 52-59).

17. Regarding claim 17, Fielder disclosed that each proof data generation algorithm is a one-way function (See Fielder Col. 8 Lines 27-32, and Col. 10 Lines 16-27).

18. Regarding claim 18, Fielder disclosed a system for enabling a server device to validate a client device, said system comprising: at least one client device (See Fielder Fig. 1 Element 10); a server device (See Fielder Fig. 1 Element 11); a shared unpredictable secret (See Fielder Fig. 2 Element 21); means for storing the shared unpredictable secret the client device (See Fielder Fig. 1 Element 5b); means for storing the shared unpredictable secret the server device (See Fielder Fig. 1 Element 17b); coupled to client device and to server device, means for determining whether the client device holds a correct secret (See Fielder Fig. 3b Element 118 and Fig. 4b

Element 217); coupled to the determining means, means for allowing the server device to validate the client device when the client device proves that it holds a correct secret (See Fig. 3b Element 121 and Fig. 4b Elements 217-219); and coupled to the client device and to the server device, means for replacing the original shared unpredictable secret with a new shared unpredictable secret when server device validates the client device (See Fig. 3b Elements 123-124 and Fig. 4b Elements 220-221) (Also see Fielder claims 1-19).

19. Regarding claim 19, Fielder disclosed a computer readable medium containing computer program instructions for enabling a server device to validate client device (See Fielder Col. 5 Lines 63-65), said computer program instructions causing the execution of the following steps: generating a shared unpredictable secret; storing the shared unpredictable secret in the client device and in the server device; requiring the client device to prove that it holds a correct secret as a precondition to allowing the client device to be validated by the server device; and replacing the shared unpredictable secret by a new shared unpredictable secret when the client device is validated by the server device (See the rejection of claim 1 above).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

21. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fielder as applied to claim 1 above, and further in view of Yatsukawa (US Patent Number 6,148,404).

22. Regarding claim 2, Fielder disclosed both the originating computer and the answering computer as containing the original dynamic secret (See Fielder Col. 3 Paragraph 3), but failed to disclose how they both obtained the secret.

Yatsukawa teaches that in a one-time password system, a registration operation should be performed in order to determine the initial secret (See Yatsukawa Col. 15 Line 65 – Col. 16 Line 12).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Yatsukawa in the one-time password system of Fielder by having a registration step in which an initial secret was agreed upon and set in the originating and answering systems. This would have been obvious because the ordinary person skilled in the art would have bee motivated to provide a means for both the systems to contain identical secrets, as required by Fielder for the one-time password system to work properly.

23. Regarding claim 3, the combination of Fielder and Yatsukawa disclosed that a token can be activated by checking an activation code in order to use the system (See Fielder Col. 13 Paragraph 2), and also checking a user id and email address and other such information (See Yatsukawa Col. 16 Paragraph 2).

24. Regarding claim 4, the combination of Fielder and Yatsukawa disclosed that the token must be purchased (See Fielder Col. 12 Lines 64-67).

25. Claims 9, 11-12, and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fielder as applied to claim 1 above, and further in view of Menezes (Handbook of Applied Cryptography).

26. Regarding claim 9, Fielder disclosed the originating system applying a random change value to the dynamic secret in order to update the secret (See Fielder Col. 9 Paragraph 1), but failed to disclose the change value being received from the answering system.

Menezes teaches a method for in which a verifier provides a challenge value to a claimant, and the claimant applies the challenge to a known secret in which the time required to respond to the challenge is monitored (See Menezes Pages 397-399).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Menezes in the authentication system of Fielder by having the answering system create the random change value and provide it to the originating system. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against replay attacks, ensure timeliness of the reply, and therefore ensure that the originator was in fact the holder of the dynamic secret, and further to lessen the computation required of the originator, and token within.

27. Regarding claim 11, the combination of Fielder and Menezes disclosed sending acknowledgement data to the answering system to confirm that the originating system had replaced the shared secret with the new secret (See Fielder Col. 8 Paragraphs 3-5).

28. Regarding claim 12, the combination of Fielder and Menezes disclosed the answering system receiving the acknowledgement, validating the originating system, replacing the dynamic secret with the new dynamic secret (See Fielder Col. 10 paragraph 5-6).

29. Regarding claims 14 and 15, the combination of Fielder and Menezes disclosed sending proof data as acknowledgement data (See Fielder Col. 8 Paragraphs 3-4 wherein the dynamic data was the new dynamic data from the previous session).

30. Claims 10, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Fielder and Menezes as applied to claim 9 above, and further in view of Lamport, Leslie (Password Authentication with Insecure Communication).

Fielder and Menezes disclosed the change value being random and applying the change value to the dynamic secret to create a new dynamic secret (See Fielder Col. 6 Paragraph 9), and providing proof data that the originating system held the correct dynamic secret (See Fielder Col. 8 Paragraph 5), however, failed to disclose that the applying was a one-way function, and also failed to disclose that proof of any future dynamic password would suffice.

Lamport teaches a method for applying updates to a secret and verifying knowledge of the secret in which the update applied is a one-way function, and in which knowledge of any future proof, can be used to grant authentication (See Lamport Section II).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Lamport in the authentication system of Fielder and Menezes by using a one-way function to update the dynamic secret and further by allowing knowledge of any future password to grant authentication. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow a simple means for re-synchronizing the dynamic secrets held in the originating device and the answering device while protecting against replay attacks.

Conclusion

31. Claims 1-19 have been rejected.

32. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Huynh et al. (US Patent Number 6,240,184) disclosed a system for synchronizing one-time passwords between a client and a server.

b. MacKenzie et al. (US Patent Number 6,757,825) disclosed a system for mutual authentication in a network involving proof of knowledge of a one-time password.

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
2/3/05

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER